(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 July 2004 (08.07.2004)

PCT

(10) International Publication Number
WO 2004/057546 A2

(51) International Patent Classification[7]: G07F 7/00

(21) International Application Number:
PCT/EP2003/050907

(22) International Filing Date:
27 November 2003 (27.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0229918.8 20 December 2002 (20.12.2002) GB

(71) Applicant *(for all designated States except US)*: **MOTOROLA INC** [US/US]; 1303 E.Algonquin Road, Schaumburg 60196 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **KOENIG, Mathias** [DE/DE]; Carl-Benz Str 12, 65232 Taunusstein (DE).

(74) Agent: **McCORMACK, Derek J.**; Motorola European Intellectual Property Operations, Midpoint, Alencon Link, Basingstoke RG21 7PL (GB).

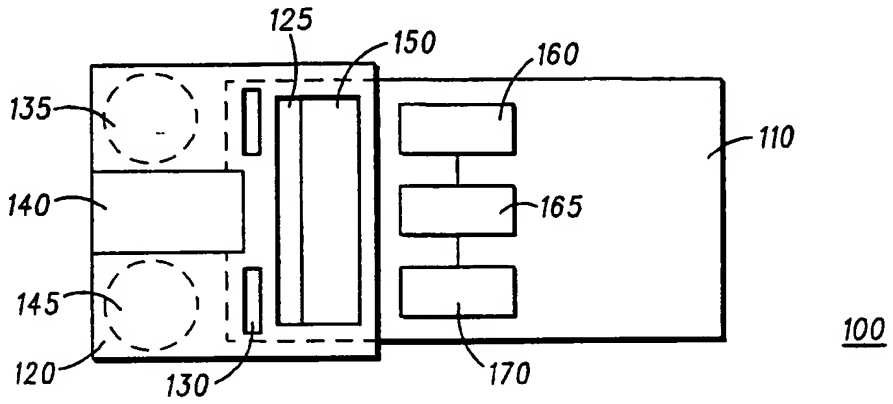
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE SMARTCARD SYSTEM AND METHOD OF OPERATION



(57) Abstract: A Smartcard (110) comprises a memory element and a charging circuit operably coupled to the memory element such that the charging circuit only provides power to the memory element for a pre-determined period of time. A portable card reader/writer (120) is provided that comprises a user authentication mechanism, for authenticating a user of a card, such as the Smartcard (110). The Smartcard reader/writer (120) initialises an operation of the Smartcard (110) in response to authenticating a user of the Smartcard (110). The provision of an authentication mechanism for a Smartcard, i.e. by requiring a user to authenticate it with a particular portable card reader/writer, significantly reduces the risk of fraudulent use of the Smartcard.

WO 2004/057546 A2

SECURE SMARTCARD SYSTEM AND METHOD OF OPERATION

Field of the Invention

This invention relates to apparatus for, and a transaction between, a portable device, such as a smart card, and a fixed device, such as a card reader/writer. The invention is applicable to, but not limited to, improving security in a Contact-less Smartcard by authenticating a user of the Smartcard.

Background of the Invention

Recent developments in wireless technology, primarily in the area of wireless local loop (WLL), have resulted in a new wireless device known as a Smartcard. Smartcards are used in a wide variety of applications. For example, it is known that Smartcards are used in electronic ticketing, time systems, and access control. Furthermore, the Smartcards are also used as a data storage function, for example containing biometric data, social security information or user profile information. In addition, Smartcards are being increasingly used in electronic purse functions such as retail, public transport ticketing, ski passport, telephone, road tolling, vending, parking and money transactions.

Current Smartcards are known to have more functionality than just memory. For example, some Smartcards are designed to communicate with a Smartcard reader/writer. In this regard, the Smartcard is designed to include a wireless interface to the reader. The type of memory used in Smartcards is also varied. For example,

Smartcards are known to include random access memory (RAM) and/or electrically erasable programmable read-only memory (EEPROM), typically used for application related data such as 'electronic-money', codes, etc. or read-only memory (ROM), typically used to store card personality data.

In the field of this invention, namely security associated with portable communication devices such as Smartcards, it is important to ensure the security of any Smartcard transaction process. In this regard, it is known that some current Smartcards utilise a Personal Identification Number (PIN), to provide security.

However, the security associated with PINs is known to be somewhat basic. User PINs are often communicated to third parties. Transactions based on the PIN can be intercepted and the PIN obtained. Also, a user's PIN may be guessed, or a third party may see what PIN a user is entering into the Smartcard. Thus, the use of PINs, in isolation, is a very limited form of security. Such use is likely to be unacceptable in future communication/ transactions that will include sensitive financial information.

An enhancement to the provision of basic PIN-based security is the use of cryptographic authentication of both the portable device (e.g. the Smartcard) and the receiving terminal (card reader). Consequently, the concept of Mutual authentication between the portable device and the fixed device has been increasingly used in the Smartcard industry.

Furthermore, it is known that the uniqueness and the non-reproducibility of the cryptographic key, as used to certify the authenticity of the overall transaction, needs to be guaranteed. As such, the concept of Cryptographic Signature (cryptographic key) has been widely used in the Smartcard industry as a reliable means to authenticate messages or transactions.

To complement this authentication process, a random session key, as opposed to a static key, is sometimes used to improve the security of the cryptographic operation involved. This makes a replay attack by a third party much more difficult. The current proposals for improving Smartcard security are focussed on asymmetric public key coding, for example, where one public key and one private key are used simultaneously.

A transaction is implemented as a critical section. The critical section commences, after a successful completion of the mutual authentication. The critical section is completed with a successful verification of the transaction signature. In such transactions, it is known that the integrity of the data stored in the portable device is an important design criterion.

Nevertheless, this approach to Smartcard transaction is still recognised as being prone to security breaches. Even the most secure Smartcard technology suffers from the fact that the Smartcards may be stolen and the card manipulated to enable an unauthorised person to use and/or take advantage of the card.

Thus, there exists a need in the field of the present invention to provide a Smartcard transaction mechanism, a Smartcard/portable device, a Terminal (card reader) and methods to initialise a Smartcard and enable a Smartcard transaction wherein the abovementioned disadvantages may be alleviated.

Statement of Invention

In accordance with a first aspect of the present invention, there is provided a Smartcard, as claimed in Claim 1.

In accordance with a second aspect of the present invention, there is provided a portable card reader/writer, as claimed in Claim 7.

In accordance with a third aspect of the present invention, there is provided a Smartcard authentication and/or initialisation system, as claimed in Claim 16.

In accordance with a fourth aspect of the present invention, there is provided a method of initialising an operation of a Smartcard, as Claimed in Claim 19.

In accordance with a fifth aspect of the present invention, there is provided a Smartcard, as claimed in Claim 24.

In accordance with a sixth aspect of the present invention, there is provided a portable card reader/writer, as claimed in Claim 25.

In accordance with a seventh aspect of the present invention, there is provided an integrated circuit adapted for use in a Smartcard or portable card reader/writer, as claimed in Claim 26.

In summary, the inventive concepts described herein propose, inter alia, an improved Smartcard security architecture, preferably for use in Contact-less environments. The improved Smartcard security system comprises a Smartcard and a portable card reader/writer configured to self-authenticate a user of the Smartcard prior to initialising the Smartcard for temporary use.

Brief Description of the Drawings

Exemplary embodiments of the present invention will now be described, with reference to the accompanying drawings, in which:

FIG. 1 illustrates a plan view of a functional block diagram of a Smartcard inserted into a portable card reader/writer used for self-authentication purposes in accordance with a preferred embodiment of the invention.

FIG. 2 illustrates a side view of the functional block diagram of FIG. 1 in accordance with a preferred embodiment of the invention.

FIG. 3 illustrates a flow of information between a Smartcard and a portable card reader/writer in accordance with a preferred embodiment of the invention.

FIG. 4 is a flowchart illustrating a preferred mechanism of self-authenticating and initialising a Smartcard using a portable card reader/writer in accordance with a preferred embodiment of the invention.

Description of Preferred Embodiments

Referring now to FIG. 1, a plan view of a Smartcard inserted into a portable card reader/writer for self-authentication purposes is illustrated, in accordance with a preferred embodiment of the invention. A Smartcard 110 is illustrated as being inserted into a portable card reader/writer 120. The portable card reader/writer 120 includes a display 150 for displaying various items of information relating to the Smartcard and/or the portable card reader/writer. For example, the display may be used to display financial information held on the Smartcard, or messages indicating the instructions to carry out, or progress (or otherwise) of, the Smartcard user self-authentication and/or Smartcard initialisation process.

The portable card reader/writer 120 further includes a user-input device 125, such as a keypad. The user input device 125 allows the user to enter information to the Smartcard 110 and/or the portable card reader/writer 120. For example, if one or more personal identification number(s) (PIN) is used, the keypad enables the PIN to be entered. In the preferred embodiment of the present invention, the portable card reader/writer also includes an optional 'menu' button. A user preferably uses the 'menu' button to manoeuvre around the screen on the display 150, or select displayed information/options.

The portable card reader/writer 120 also includes a voltage supply 145. The (battery) voltage supply 145 is used to power the portable card reader/writer as well as charge the Smartcard 110. Advantageously, the Smartcard is only charged whilst operably coupled to the portable card reader/writer 120 for a period of time after the Smartcard 110 has been inserted into the portable card reader/writer 120.

After successful completion of the authentication process, and removal of the Smartcard 110 from the portable card reader/writer 120 (and thereby its voltage supply 145), the Smartcard is configured to lose its charge. A timer circuit 170, for example a resistor-capacitor (R-C) circuit operably coupled to a random access memory (RAM) 165, preferably dictates the time it takes for the Smartcard 110 to lose its charge, i.e. the charging capacitor provides a predefined voltage drop versus time.

In this manner, some of the Smartcard's functionality remains within the Smartcard for a predetermined time after:

(i) The user of the Smartcard 110 has been authenticated by the portable card reader/writer 120;

(ii) The Smartcard has been initialised by the portable card reader/writer 120; and

(iii) The Smartcard has been removed from the portable card reader/writer 120.

It is within the contemplation of the invention that, in an alternative embodiment, a digital timer circuit may be used, instead of the R-C network shown in FIG. 3. In this configuration, it is envisaged that a user is able to control/set the timer period, via the keypad 125 on the portable card reader/writer 120. In this manner, the user is able to select an appropriate time period for any particular application, for example a longer time period to access a series of secure areas, before the Smartcard 110 is to lose its functionality.

It is envisaged that a variety of Smartcard user self-authentication mechanisms can be used in the preferred embodiment. For example, the preferred user authentication mechanisms include fingerprint recognition by means of a fingerprint sensor 140 and/or voice recognition by means of microphone 135 coupled to a speech analysis processor (not shown).

In accordance with the preferred embodiment of the present invention, the portable card reader/writer 120 comprises one or more Smartcard user self-authentication modules. A first Smartcard user self-authentication process is performed, in order to activate the Smartcard 110 for a desired transaction. Preferably, the first Smartcard user self-authentication process comprises fingerprint recognition as one of the self-authentication modules, where the module includes a fingerprint sensor 140.

In this regard, the Smartcard owner places a finger onto a fingerprint sensor in order to validate the user as

being approved to use the Smartcard 110. The subsequent validation process is described later with respect to FIG. 3 and FIG. 4.

In a similar manner, a second (alternative or additional) voice recognition process, using the microphone 135 and speech processing circuitry, can be used as a self-authentication mechanism. It is envisaged that speech recognition circuitry usually found in tabletop telecommunications or computing devices can be re-used in the portable card reader/writer.

In addition, a new Smartcard device is used, which comprises internal digital electronics, for example a microprocessor 160 and a memory element 165, such as non-volatile random access memory (NV-RAM). In accordance with the preferred embodiment of the present invention, a portion, or the whole, of the NV-RAM 165 is only supplied with a voltage supply upon successful completion of the authentication process. Otherwise, the portion, or the whole, of the NV-RAM 165 is not provided with power and therefore loses any stored information.

Alternatively, it is envisaged that a number of memory elements can be provided in the Smartcard, for example read-only memory (ROM), electrically erasable ROM (EEPROM), standard RAM, etc. In this regard, the authentication process is concerned only with activating and using the NV-RAM of the Smartcard. Thus, other user-specific data, which is permanently or semi-permanently stored on the Smartcard, is not lost whenever the portable card reader/writer has been removed and the Smartcard's charge has dissipated.

In accordance with a preferred embodiment of the present invention, the proposed portable card reader/writer 120 is incorporated into for example a key ring, or infrared security key, say, for a car door. It is also envisaged that the portable card reader/writer is of such a small size that it may be readily carried inside a wallet, a purse or small enough to be carried in a user's pocket etc.

In this regard, it is envisaged that the portable card reader/writer is configured as a 'slim' device, as represented in the side view illustration in FIG. 2. In such a configuration, it is envisaged that the electronic circuitry of the portable card reader/writer 120 may be incorporated onto a flexible printed circuit board for electrically coupling to, or wrapping around, the Smartcard 110 when it is inserted into the portable card reader/writer 120.

Although the preferred embodiment of the present invention illustrates a Smartcard being inserted into the portable card reader/writer, a skilled artisan will appreciate that many other forms of mechanically and electrically coupling the two devices can be used, in order to benefit from the inventive concepts herein described. For example, in some embodiments, it is envisaged that a wireless coupling between the Smartcard and the portable card reader/writer may be used, for example using the same wireless local loop (WLL) technology used by the Smartcard in its normal operation.

FIG. 3 illustrates a flow of information between a Smartcard and a portable card reader/writer in accordance with a preferred embodiment of the invention. The flow of information effectively represents an enhanced security in the use of the Smartcard.

To be able to use the Smartcard 110 for a particular application, for example a financial transaction or access to a building, the Smartcard 110 needs to be inserted into a receptacle slot within the portable card reader/writer 120. Either by insertion of the Smartcard 110 into the receptacle slot or, for example, by pressing a menu button on a user interface 125 on the portable card reader/writer 120, the portable card reader/writer 120 will be activated. As an added security measure, it is envisaged that the portable card reader/writer may also be activated only by entering a pass (or PIN) code.

In accordance with the preferred embodiment of the present invention, the Smartcard 110 comprises one or more Smartcard user self-authentication modules. A first Smartcard self-authentication process is performed, in order to activate the Smartcard for a desired transaction. Preferably, the first Smartcard user self-authentication process comprises fingerprint recognition as one of the self-authentication modules, where the module includes a fingerprint sensor. In this regard, the Smartcard owner places a finger onto a fingerprint sensor on the portable card reader/writer 120.

A digital data management function 325, for example a micro-controller and/or processor, in the portable card reader/writer 120 compares the scanned fingerprint with a

previously stored fingerprint (i.e. one from a stored personal reference data set 315). If the scanned fingerprint matches the previously stored fingerprint with a sufficient degree of accuracy, then a number of operations are performed.

First, the Smartcard 110 is powered, via a charging/timer circuit 370, for example an R-C network. The NV-RAM of the Smartcard 110 is preferably only charged by the voltage supply 145 of the portable card reader/writer 120 following a 'match'. Once the Smartcard has been removed from the portable card reader/writer 120, the timer/charging circuit is arranged to provide a slowly dissipating supply voltage to the NV-RAM 165 of the Smartcard 110.

In addition, whilst the Smartcard is operably coupled to the portable card reader/writer 120, a user specific codeword is then transferred from the digital data management 325 of the portable card reader/writer to a specific portion of memory 365, such as NV-RAM, of the Smartcard 110. This transfer is performed via the Smartcard's digital data management function 350. Preferably, the codeword is specific to the particular portable card reader/writer 120.

The charging capacitor comprises part of, or is preferably operably coupled to, a timing circuit within the Smartcard 110. Such timing/charging circuits 370 are well known in the general field of electronics. In this regard, the charging capacitor retains its power for a predefined period of time. In this manner, the NV-RAM is

only configured to hold the specific codeword for this predefined time.

Consequently, the Smartcard user has been self-authenticated in the portable card reader/writer 120. The self-authentication mechanism is configured to last a predetermined period of time. Thus, once authenticated, the card owner is able to perform the desired Smartcard action, for example, a bank transaction or enter a secure area only within this predefined time.

After the predefined time has elapsed, the charging capacitor effectively loses its power. Consequently, the NV-RAM 365 loses its power and the specific codeword within the Smartcard 110 is lost. Advantageously, this self-authentication mechanism provides substantial additional security, as the Smartcard 110 cannot be used for any subsequent transaction until the above described self-authentication process is repeated.

It is within the contemplation of the invention that, instead of, or in addition to, the fingerprint recognition mechanism 305, a PIN can be entered on the portable card reader/writer 120. Furthermore, it is envisaged that a second PIN may be used, whereby the second PIN may be entered on the Smartcard if it is configured with its own user input, such as a keypad (not shown).

It is also within the contemplation of the invention that alternative self-authentication modules can be used, to enhance the security of the Smartcard system. For example, as an alternative, or in addition, to the

fingerprint recognition and/or PIN arrangement, voice recognition may be used. In this manner, a voice recognition module, operably coupled to say a built-in microphone within the portable card reader/writer, compares the spectral properties of a user's received voice input with a stored spectral voice signal for that user. The aforementioned Smartcard initialisation processes of power and codes routed to the Smartcard are performed upon the portable card reader/writer determining a 'match' of the speech signal.

Notably, and in particular when a combination of self-authentication modules is used, increased security can be achieved.

It is also within the contemplation of the invention that the Smartcard and associated portable card reader/writer may be inexorably linked, inasmuch as they are a ('matched-pair' and are only configured to work with each other. For example, in this context, an additional code may be provided within the Smartcard, which is only recognised by its portable card reader/writer. In this manner, the security between the Smartcard and the portable card reader/writer is further enhanced.

In an enhanced embodiment of the present invention, the digital data management function 325 of the portable card reader/writer 120 is configured to extract information from the Smartcard 110, and display Smartcard information to the user. The portable card reader/writer user is able to read out, for example, financial or other information from the Smartcard 110. This is specifically useful in the case where a prepaid or preloaded Smartcard

110 is used, where the user is likely to be keen to know how much money is available on the Smartcard 110.

It is within the contemplation of the invention that the aforementioned Smartcard system may be used as an add-on security feature to current digital signature technologies, such as asymmetric public key coding where one public key and one private key are used.

It is also envisaged that an additional advantageous feature of the present invention is the provision of a Bluetooth ™ and/or infrared transceiver within the portable card reader/writer and/or Smartcard. In this regard, the portable card reader/writer is preferably configured to communicate with, say, a wireless phone, a computer and/or the Internet. With such a configuration, it is possible for a user to effect, say, a bank transaction whilst sitting in a car in front of a bank.

Referring now to FIG. 4, a preferred flowchart 400 for self-authentication of a Smartcard is illustrated. The preferred method commences when the Smartcard is plugged into a portable card reader/writer, in step 405. After inserting the Smartcard into the portable card reader/writer in step 405, the micro-controller operation is commenced in both the portable card reader/writer and in the Smartcard, as shown in step 410.

The preferred method for commencing the respective micro-controller operations is by, say, a user pressing a button on the portable card reader/writer. Alternatively, it is envisaged that the micro-controller

may by activated by the user just plugging the Smartcard into the portable card reader/writer.

Once the respective micro-controllers have been activated in step 410, one or more Smartcard user self-authentication processes are commenced as shown in step 415. A preferred user-authentication process is fingerprint recognition, whereby a user is able to press a finger onto the fingerprint sensor. Alternatively, other user-authentication processes can be used, such as voice recognition whereby a user utters a codeword into the microphone and/or typing in a PIN.

The portable card reader/writer data management/ micro-controller then compares the user input to a previously stored user-authentication user input, i.e. fingerprint, voice recognition spectral pattern or PIN. The stored user-authentication input is termed a Personal Reference Data Set (PRDS) stored in the portable card reader/writer. If the comparison yields a ‚match', in step 420, then the portable card reader/writer transfers appropriate data to the Smartcard's micro-controller, as shown in step 425. The appropriate data may include one or more PINX number to be sent to the Smartcard.

In this regard, a PINX number can be considered as an extension to a PIN number. The PINX number may be a number that is generated from any series of numbers (PIN, codes or any user-entered number) from the Smartcard and/or Smartcard reader/writer. Thus, use of a PINX number further increases security in the use of the Smartcard.

The Smartcard micro-controller calculates the final codeword from the PINX (plus the PIN number) and the internal fixed codeword (IFC). The Smartcard micro-controller saves the codeword(s) into its NV-RAM cell. Furthermore, the Smartcard is preferably powered from the portable card reader/writer once the Smartcard user has been authenticated. The Smartcard is then preferably removed from the portable card reader/writer, in step 430.

Now the portable card reader/writer automatically switches itself off, in step 435. A timer in the Smartcard is then activated. The timer may take any form, for example a simple resistor-capacitor (R-C) charging circuit. Whilst the timer has not exceeded a threshold, i.e. the timer has not elapsed, the Smartcard remains in an active operational mode. For example, it is envisaged that the R-C charging/timer circuit may be set for approximately ninety seconds, to allow the Smartcard user enough time to access a building using the active Smartcard or perform a financial transaction, as shown in step 440.

It is envisaged that plugging the Smartcard into an automatic teller machine slot may effect such a transaction. Alternatively, it is envisaged that in the case of an optional radio frequency (RF) link (i.e. for a contact-less Smartcard) the user only needs to be in the vicinity of the banking machine.

After the Smartcard NV-RAM cell timer has elapsed, the Smartcard's operational mode is terminated, i.e. it is no longer capable of performing a financial transaction

without re-starting the whole process with the portable card reader/writer again. Advantageously, if the Smartcard is subsequently stolen or manipulated after the timeout, no subsequent transaction is possible. Thus, for subsequent transactions to occur a user is required to authenticate the Smartcard with its portable card reader/writer again. In this manner, a user has to be in possession of the portable card reader/writer *and* the associated Smartcard *and* be authorised to use the Smartcard as described above.

Furthermore, in accordance with the preferred embodiment of the present invention, the disclosure or theft of a PIN number is not sufficient to allow a third party to fraudulently use the Smartcard, if the PIN mechanism is used with another user-authentication process.

It will be understood that the Smartcard system, the Smartcard/portable device, the portable card reader/writer (Terminal) and methods to enable authentication and initialisation of a Smartcard, as described above, tend to provide at least one or more of the following advantages:

(i) The provision of an authentication mechanism for a Smartcard, i.e. by requiring a user to authenticate himself/herself with a particular portable card reader/writer, significantly reduces the risk of fraudulent use of the Smartcard.

(ii) The provision of a user authentication mechanism within the portable card reader/writer, prior to subsequently authorising the Smartcard, i.e. by

requiring a user to undergo fingerprint analysis, voice recognition or entering a PIN, further significantly reduces the risk of fraudulent use of the Smartcard.

(iii) The provision of a mechanism to 'charge' the Smartcard only after a coupling the Smartcard to the portable card reader/writer and/or following authentication of the Smartcard, i.e. by incorporating a mechanism for the particular portable card reader/writer to charge a NV-RAM in the Smartcard. This further significantly reduces the risk of fraudulent use of the Smartcard.

(iv) The provision of a predetermined short time limit for any authentication of the Smartcard, i.e. by incorporating a charge dissipation mechanism in the Smartcard, further significantly reduces the risk of fraudulent use of the Smartcard.

(v) The proposed system is backward compatible, in that it is able to enhance existing Smartcard systems, as well as provide increased security to future Smartcard systems.

(vi) The provision of a display on the portable card reader/writer allows a user to view data and/or codes of the Smartcard and/or portable card reader/writer. A user is also able to receive instructions/messages on the self-authentication and/or Smartcard initialisation processes.

It will, of course, be understood that a Smartcard or portable card reader/writer, as described above, will

typically be constructed around one or more integrated circuits that are adapted to provide the required functionality described above.

Whilst specific, and preferred, implementations of the present invention are described above, it is clear that one skilled in the art could readily apply variations and modifications of such inventive concepts.

Thus, a transaction system, Smartcard/portable device, Terminal and methods of performing a transaction have been provided whereby the problems associated with prior art arrangements have been substantially alleviated.

Claims

1. A Smartcard (110) comprising a memory element (165), the Smartcard (110) characterised by a charging circuit (170) operably coupled to said memory element(165) such that the charging circuit (170) only provides power to said memory element (165) for a pre-determined period of time.

2. The Smartcard according to Claim 1, wherein the memory element is a non-volatile random access memory.

3. The Smartcard according to Claim 1 or Claim 2, wherein said charging circuit is operably coupled to an external power source that provides power to said charging circuit.

4. The Smartcard according to Claim 3, wherein said external power source is within a portable card reader/writer, such that said external power source provides power to said charging circuit when said portable card reader/writer is operably coupled to said Smartcard.

5. The Smartcard according to Claim 3 or Claim 4, wherein said external power source is located within a portable card reader/writer, such that said external power source provides power to said charging circuit after a Smartcard user has been authenticated to use said Smartcard.

6. The Smartcard according to any preceding Claim, the Smartcard further characterised in that the charging

circuit comprises, or is operably coupled to, a timer circuit such that said timer circuit controls the period of time that the memory element is provided with power.

7. A portable card reader/writer (120) for interfacing with at least one card, for example a Smartcard (110), wherein the portable card reader/writer (120) is characterised by a user authentication mechanism, for authenticating a user of said card.

8. The portable card reader/writer according to Claim 7, wherein the portable card reader/writer is further characterised by a memory element, operably coupled to the user authentication mechanism, which stores user authentication data.

9. The portable card reader/writer according to Claim 8, wherein the portable card reader/writer is further characterised by a processor, operably coupled to the memory element and the user authentication mechanism, such that in order to authenticate a user the processor compares user data provided by the user authentication mechanism with user data stored in the memory element.

10. The portable card reader/writer according to any of preceding Claims 7 to 9, wherein the portable card reader/writer is further characterised by the user authentication mechanism being one or more of: a finger print authentication arrangement, voice recognition circuitry, or a user input device for entering PIN or code data.

11. The portable card reader/writer according to any of preceding Claims 7 to 10, wherein the portable card reader/writer is further characterised by a display (150) for displaying information relating to the card and/or the portable card reader/writer.

12. The portable card reader/writer according to any of preceding Claims 7 to 11, wherein the portable card reader/writer is further characterised by a voltage supply (145) configured to provide power to a Smartcard when the Smartcard is operably coupled to the portable card reader/writer.

13. The portable card reader/writer according to any of preceding Claims 9 to 12, wherein the portable card reader/writer is further characterised by said processor sending data and/or access codes to a Smartcard, when said Smartcard is operably coupled to the portable card reader/writer.

14. The portable card reader/writer according to any of preceding Claims 9 to 13, wherein the portable card reader/writer is further characterised by a user-input device (125), such as a keypad, to enable a user to enter information to the portable card reader/writer and/or a Smartcard (110) operably coupled to the portable card reader/writer (120).

15. The portable card reader/writer according to any of preceding Claims 7 to 14, wherein the portable card reader/writer is further characterised by a communication transmitter and/or receiver for communicating with a remote communication system, wherein the communications

with the remote system are performed using Bluetooth ™ and/or infrared communications.

16. A Smartcard authentication and/or initialisation system characterised by a Smartcard reader/writer (120) comprising a Smartcard user authentication mechanism and a Smartcard (110) for operably coupling to the Smartcard reader/writer (120) such that the Smartcard reader/write (120) initialises an operation of the Smartcard (110) in response to authenticating a user of the Smartcard.

17. The Smartcard authentication and/or initialisation' system according to Claim 16, further characterised in that said Smartcard reader/writer initialises an operation of the Smartcard by transferring a user-specific or Smartcard-specific codeword to the Smartcard (110).

18. The Smartcard authentication and/or initialisation system according to Claim 16 or Claim 17, further characterised in that said Smartcard reader/writer and said Smartcard comprise one or more of the following communication mechanisms to communicate with each other or a remote communication unit: a wireless local loop communication link, a Bluetooth ™ communication link, an infrared communication link.

19. A method of initialising an operation of a Smartcard, the method comprising the steps of:

entering user information into a portable card reader;

authenticating whether said user information matches a user of said Smartcard; and

initialising an operation of said Smartcard in response to a positive authentication.

20. The method of initialising an operation of a Smartcard according to Claim 19, wherein said step of authenticating comprises the step of:

comparing a user input to a previously stored user-authentication user input, wherein said user input is one or more of: a fingerprint, a voice signal, a PIN code.

21. The method of initialising an operation of a Smartcard according to Claim 19 or Claim 20, wherein said step of initialising comprises the step of:

transferring financial or access code data to the Smartcard.

22. The method of initialising an operation of a Smartcard according to any of preceding Claims 19 to 21, wherein said step of authenticating comprises the step of:

providing power to the Smartcard from the portable card reader/writer once the Smartcard user has been authenticated.

23. The method of initialising an operation of a Smartcard according to Claim 22, wherein said step of initialising comprises the step of:

providing power to a memory element within said Smartcard for a limited period of time.

24. A Smartcard adapted for use in the method steps of any of the preceding Claims 17 to 23.

25. A Portable card reader/writer adapted for use in the method steps of any of the preceding Claims 17 to 23.

26. An integrated circuit adapted for use in a Smartcard according to any one of preceding claims 1 to 6, or in a portable card reader/writer according to any one of preceding Claims 7 to 15.

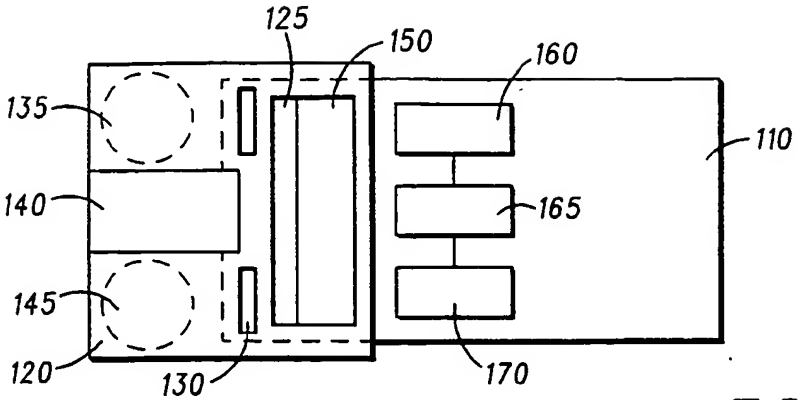


FIG. 1

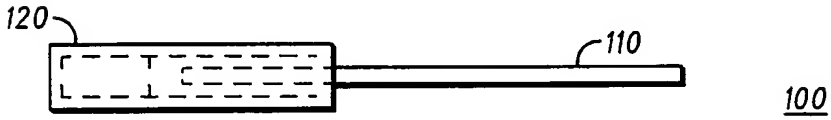


FIG. 2

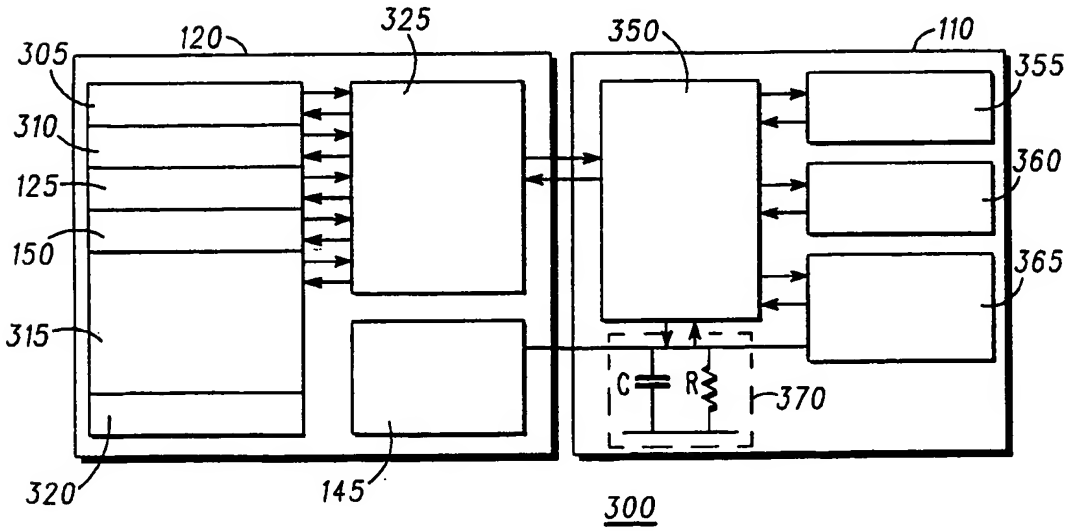


FIG. 3

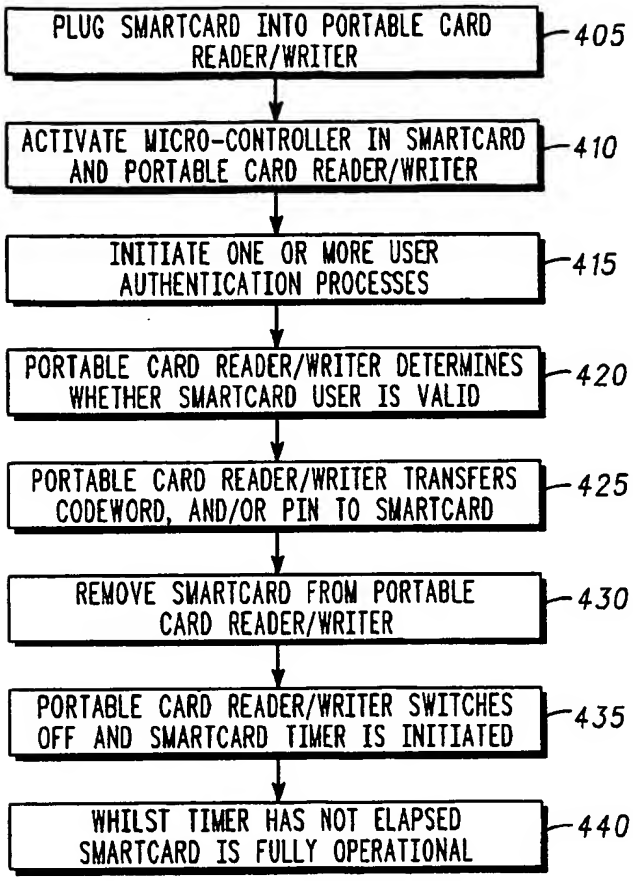

PLUG SMARTCARD INTO PORTABLE CARD READER/WRITER
405
ACTIVATE MICRO-CONTROLLER IN SMARTCARD AND PORTABLE CARD READER/WRITER
410
INITIATE ONE OR MORE USER AUTHENTICATION PROCESSES
415
PORTABLE CARD READER/WRITER DETERMINES WHETHER SMARTCARD USER IS VALID
420
PORTABLE CARD READER/WRITER TRANSFERS CODEWORD, AND/OR PIN TO SMARTCARD
425
REMOVE SMARTCARD FROM PORTABLE CARD READER/WRITER
430
PORTABLE CARD READER/WRITER SWITCHES OFF AND SMARTCARD TIMER IS INITIATED
435
WHILST TIMER HAS NOT ELAPSED SMARTCARD IS FULLY OPERATIONAL
440
400

FIG. 4